OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

Privacy Policies and Procedures

Ruth Marks and Stacey Pratt
Access and Privacy Analyst
April 2019

Agenda

- Privacy and the *ATIPPA, 2015.*
- Review of Privacy Management Programs.
- Development of policies and procedures.
- Understanding of continuing commitment to compliance.

Privacy and the *ATIPPA, 2015*

- Part III of the *ATIPPA, 2015* - Protection of Personal Information.
- Privacy under the *ATIPPA, 2015* involves the protection of personal information from unauthorized collection, use and disclosure.
- Persons who believe there has been an unauthorized collection, use or disclosure of their personal information may file a complaint with the OIPC.

Privacy Management Program

- Developing a Privacy Management Program ("PMP") will assist public bodies in:
  - ensuring legislative compliance; and
  - demonstrating accountability.
- Why is a PMP necessary?
  - Established legislative expectations.
  - OIPC investigations.
  - Risks (privacy breaches, privacy complaints, investigations, audits, offences).
- Policies and procedures are key components of a robust PMP.

Policies and Procedures

- Policies and procedures are one way to demonstrate:
  - a general commitment to privacy;
  - ability to manage a privacy breach should one occur; and
  - compliance with section 64 of the *ATIPPA, 2015.*

Policies and Procedures

- The Protection of Privacy Policies and Procedures Manual from the ATIPP Office sets out the legislative requirements.
- Public bodies must review these requirements and consider:
  - How do they apply in your organization?
  - Do you have organization-specific policies and procedures?
  - Do you have policies and procedures for specific programs and initiatives?
  - Has a copy been made available to staff?
  - Have staff been trained on the policies and procedures? If so, is this training documented?

Necessary Policies and Procedures

- Organizations should develop and maintain privacy policies, including policies covering:
  - the collection of personal information, including consent;
  - access to, correction of and accuracy of personal information;
  - the retention and secure destruction of personal information;
  - the requirements for administrative, technical and physical safeguards;
  - the process for managing privacy-related complaints; and
  - the process for responding to a privacy breach.

Collection of Personal Information

Legislative Requirements - Notification

62 (2) A public body shall tell an individual from whom it collects personal information

(a) the purpose for collecting it;
(b) the legal authority for collecting it; and
(c) the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.

Legislative Requirements - Consent

66. (1) A public body may use personal information only (b) where the individual the information is about has identified the information and has consented to the use, in the manner set by the minister responsible for this Act;

68. (1) A public body may disclose personal information only (b) where the individual the information is about has identified the information and consented to the disclosure in the manner set by the minister responsible for this Act;

Policy Details

- These policies will describe:
  - direct versus indirect collection;
  - collection of the minimum necessary PI;
  - when notice of the collection is required and how the notice is given, including a discussion of the authority for the collection;
  - if consent is the authority for collection:
    - the methods for obtaining consent and the content of the consent form;
    - the process for authorizing and verifying personal representatives;
  - the contact person for collection-related issues or concerns.

Be Prepared to Discuss

- Acceptable reasons for collecting personal information.
- Acceptable uses of personal information.
- Disclosure:
  - When disclosure is permitted – both to persons and other organizations – and how this disclosure must occur.
  - The elements of consent.
  - Disclosure of non-identifiable information.
  - Maintaining a record of disclosure.

Program-Specific Policies

- Examples:
  - A social worker may indirectly collect personal information about an individual from a physician or law enforcement.
  - One time indirect collection of personal information by the Department of Health and Community Services during a pandemic.

Access to, Correction of and Accuracy of Personal Information

Legislative Requirements - Access and Correction

8(1) A person who makes a request under section 11 has a right of access to a record in the custody or under the control of a public body, including a record containing personal information about the applicant.

10(1) An individual who believes there is an error or omission in his or her personal information may request the head of the public body that has the information in its custody or under its control to correct the information.

Policy Details

- These policies will address both informal and formal requests.
- Formal – processed through the ATIPP Coordinator in compliance with *ATIPPA, 2015.*
- Informal – routine access and correction.
  - Answering particular questions.
  - Specifying categories of records for routine release.
  - Active publication/dissemination.

Policy Details

- The informal request policy should describe:
  - the process for responding to informal access requests;
  - the process for routine disclosures; and
  - the process for responding to informal correction requests.
- The formal request policy should describe:
  - the process and timeframes for requests from individuals for access to their own personal information; and
  - the process and timeframes for requests for the correction of personal information.

Legislative Requirements - Accuracy

63. Where an individual's personal information will be used by a public body to make a decision that directly affects the individual, the public body shall make every reasonable effort to ensure that the information is accurate and complete.

Policy Details

- These policies should describe:
  - the commitment to ensuring the accuracy of personal information used to make decisions about an individual;
  - the steps that will be taken to ensure accuracy during collection; and
  - the process for reviewing personal information holdings and how and when that personal information is updated.

Be Prepared to Discuss

- If and why a formal request is required.
- Where to locate details of the information holdings of the public body, including the identity and contact information of the individual that can assist with same.
- The concept of a personal representative and the process for determining who is a personal representative.
- Timelines and potential outcomes.
  - Very important to manage expectations.

Retention and Secure Destruction of Personal Information

Legislative Requirements - Retention and Disposal

65.(1) Where a public body uses an individual's personal information to make a decision that directly affects the individual, the public body shall retain that information for at least one year after using it so that the individual has a reasonable opportunity to obtain access to it.

(2) A public body that has custody or control of personal information that is the subject of a request for access to a record or correction of personal information under Part II shall retain that information for as long as necessary to allow the individual to exhaust any recourse under this Act that he or she may have with respect to the request.

Policy Details

- These policies should:
  - classify types of records;
  - prescribe how long each type of record are kept;
  - describe the process for securely disposing of records once they are no longer needed;
  - Document reasonable safeguards throughout life cycle of the record (which may differ based on the sensitivity of the information); and
  - include references to any statutory records retention and disposition schedules that must be followed.

Policy Details

- Consider whether the policies needs to address specific circumstances:
  - Were commitments made at the time of collection for individual programs and initiatives?
  - Do different categories of records require different safeguards? How does this affect day-to-day operations?

Be Prepared to Discuss

- How the retention and destruction schedule meets collection commitments, as well as organizational and legislative requirements.
- The impact of:
  - access or correction requests;
  - the use the information to make a decision that directly impacts individual; and
  - updates to the accuracy of the information.
- Transitory records.

Requirements for Administrative, Technical and Physical Safeguards

Legislative Requirements - Safeguards

64.(1) The head of a public body shall take steps that are reasonable in the circumstances to ensure that

(a) personal information in its custody or control is protected against theft, loss and unauthorized collection, access, use or disclosure;

(b) records containing personal information in its custody or control are protected against unauthorized copying or modification; and

(c) records containing personal information in its custody or control are retained, transferred and disposed of in a secure manner.

Policy Details

- These policies should discuss all types of safeguards employed to protect personal information.
- Safeguards include:
  - physical measures, for example, locked filing cabinets and restricted access to offices;
  - administrative measures, for example, security clearances and limiting access on a “need-to-know” basis; and
  - technological measures, for example, the use of passwords and encryption.

Policy Details

- These policies should describe:
  - the physical and administrative measures taken to secure personal information both in paper and electronic form;
  - the technical steps taken to secure network and communications infrastructure;
  - the process for identifying and verifying users of personal information;
  - deciding what personal information staff need to use to carry out their duties;
  - acceptable uses of personal information; and
  - how changes are made when users change positions or leave.

Be Prepared to Discuss

- Different levels of safeguards for different personal information, programs and/or information banks.
- The specific details of the safeguards.
  - Example – encryption. Is the information encrypted during transmission, on the server or both?
- How safeguards meet expectations stemming from collection commitment.
- Tools available to staff for compliance.
  - Must be practical to be achievable.

Be Prepared to Discuss

- Access – who has access to what information and why.
- Organization-specific policies and procedures.
  - If relying on organization-wide policies and procedures, you need to be familiar with them. For example, if a government department is relying OCIO's policy regarding logout times, the department must know OCIO's default times.

Managing Privacy-related Complaints

Legislative Requirements - Access or Correction Complaint

42. (1) A person who makes a request under this Act for access to a record or for correction of personal information may file a complaint with the commissioner respecting a decision, act or failure to act of the head of the public body that relates to the request.

Legislative Requirements - Privacy Complaint

73. (1) Where an individual believes on reasonable grounds that his or her personal information has been collected, used or disclosed by a public body in contravention of this Act, he or she may file a privacy complaint with the commissioner.

(2) Where a person believes on reasonable grounds that personal information has been collected, used or disclosed by a public body in contravention of this Act, he or she may file a privacy complaint with the commissioner on behalf of an individual or group of individuals, where that individual or those individuals have given consent to the filing of the privacy complaint.

(3) Where the commissioner believes that personal information has been collected, used or disclosed by a public body in contravention of this Act, the commissioner may on his or her own motion carry out an investigation

Policy Details

- These policies should support a prompt and appropriate response to complaints and include:
  - the identification of lead;
  - a description of the investigative process;
  - the process for communicating with:
    - management;
    - the complainant, including informing of the OIPC's authority to investigate if a breach is found to have occurred; and
    - the OIPC.

Be Prepared to Discuss

- Individuals have a right to complain, even if it appears frivolous or vexatious on the surface.
- Expectation that all necessary staff participate in the investigation process.
- Potential HR implications.
- Process for determining root cause.
- Requesting resources to address issues:
  - Training.
  - Other.
- Examining complaints as a means of assessing effectiveness of overall program.

Managing Privacy Breaches

Legislative Requirements

64. (3) Except as otherwise provided in subsections (6) and (7), the head of a public body that has custody or control of personal information shall notify the individual who is the subject of the information at the first reasonable opportunity where the information is

(a) stolen;

(b) lost;

(c) disposed of, except as permitted by law; or

(d) disclosed to or accessed by an unauthorized person.

(4) Where the head of a public body reasonably believes that there has been a breach involving the unauthorized collection, use or disclosure of personal information, the head shall inform the commissioner of the breach.

Policy Details

- These policies should define “breach of personal information” and detail how staff report a breach.
- These policies should support a prompt and appropriate response to breaches and include:
  - the identification of lead;
  - a description of the containment, mitigation and overall investigative process;
  - the process for communicating with:
    - management;
    - impacted individuals (if deemed appropriate and/or required); and
    - the OIPC.

Be Prepared to Discuss

- Importance of recognizing and reporting breaches, as well as consequences of not reporting.
- Expectation that all necessary staff participate in the containment, mitigation and investigation process.
- Potential HR implications.
- Process for determining root cause.
- Need to review existing resources, such as policies, to determine if changes required.
- Examine breaches as a means of assessing effectiveness of overall program.

I've got policies!
I'm done, right?

Training and Awareness

- Lack of awareness causes breaches.
- Employees should participate in on-going mandatory privacy education (training and awareness).
- Provide knowledge and understanding of policies and procedures for all aspects of privacy protection.
- Goal for all employees is to recognize and address issues as they arise and create a culture of privacy.
- Educational tracking is also useful if a complaint or breach occurs.

Training and Awareness

- Consider a policy and affiliated procedures regarding training and awareness.
- Policy should consider:
  - Training requirements and timing.
    - May vary based on exposure to PI.
  - Frequency.
  - Tracking.
  - Mandatory nature.
  - Awareness activities.
  - Responsibility for compliance.

Procedures

- Several sections of the PMP guidance piece reference procedures:
  - Privacy and Security Risk Assessment;
  - Information Sharing Agreements; and
  - Transparent communication with individuals.
- Important to ensure consistency, clear responsibilities and establish expectations.

Oversight and Review

- Conduct random audits to determine compliance with policies and procedures.
- Work with managers and HR staff to identify problem areas.
- Investigate privacy breaches to ensure root cause addressed.
- Compile thorough reports to establish due diligence.
- Effectively communicate to employees any changes to processes or policy.
- Reach out to external agencies to assist in addressing concerns. (e.g. OIPC, ATIPP Office, governing organization, etc.)

Tips

- Need to hear messages an average of three times before it is remembered.
- Explain why – involve staff in the process when possible.
  - Buy-in is critical.
- Identify and highlight change champions and those resisting the change.
- Find ways to make the culture shift as simple and effective as possible.
- Policies and procedures should be detailed but use plain language
- Consider posting appropriate policies and procedures on your website; proactive disclosure

Questions